Indonesian Journal of Electrical Engineering and Computer Science
Vol. 20, No. 1, October 2020, pp. 545~551
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v20.i1.pp545-551

An efficient hybrid model for secure transmission of data by using efficient data collection and dissemination (EDCD) algorithm based WSN

Mustafa Mahmood Akawee[1], Mohanad Ali Meteab Al-Obaidi [2], Haider Mohammed Turki Al-Hilfi[3] Sabbar Insaif Jassim[4],Tole Sutikno[5]
[1]Department of Theology, The Great Emam University College, Iraq
[2]Al-Mustansiriya University, College of Science, Department of Computer Science, Iraq
[3]Directorate General of Vocational Education, Ministry of Education, Iraq
[4]Faculty of Al-dour Technical institute, Northern Technical University, Iraq
[5]Department of Electrical Engineering, Universitas Ahmad Dahlan, Indonesia
[5]Embedded System and Power Electronics Research Group (ESPERG), Indonesia

Article Info

Article history:

Received Jan 20, 2020
Revised Mar 22, 2020
Accepted Apr 2, 2020

Keywords:

Data collection
Energy consumption
Rivest–shamir–adleman
security
Wireless sensor network

ABSTRACT

Wireless sensor network is the life wire of the internet of things (IoT) paradigm. One of themajor issues in IoT and WSN is energy consumption owing to the consumption of energy by the security gadgets in the newtork. Solving the security-related issues for the transmitted data using IoT sensor node also involves energy consumption and this ads to the already existing energy-relatd problem in the system. With these considerations, it seems difficult to find solutions that can achieve satisfactory reduction of energy consumption while maintaing the expected level of system security and services. Therefore, in this paper, we proposed an efficient hybrid model for secure transmission of data from sensor nodes to receivers in WSN applications. The proposed model includes two algorithms Rivest–Shamir–Adleman (RSA) and efficient data collection and dissemination (EDCD). The key idea behind the proposed model is to prevent to secure sensed data if no significant change between the current data and the last transmitted data by the apply EDCD1 algorithm, which that will help in saving the sensor node energy. The reason for that the size of cipher data is so large compared to the sensed data, which that will increase the energy consumption. The outcome results shown that the proposed model has a high performance compared to RSA in term of energy consumption

Corresponding Author:

Mustafa Mahmood Akawee.
Department of Theology,
The Great Emam University College, Baghdad, Iraq
Email: it.diyala2@gmail.com

1. INTRODUCTION

Due to the unique challenges brought about by "sensor networks, traditional security technologies used in traditional networks cannot be applied directly" [1, 2]. First, the sensor network is economically profitable because the energy, computing and communication capabilities of the sensor device are limited. Second, sensor nodes are often deployed in inaccessible areas, increasing the risk of physical attacks [3-6]. Third, the sensor network interacts closely with the physical environment and personnel and constitutes a new security issue. WSN is "one of the most important elements of the internet of things (IoT) paradigm. It extends the benefits of remote access, monitoring, health, and environmental research to smart cities and smarter planets" [7]. The convergence of wireless sensor networks with other technologies has created new demands and brought a variety of security threats [8].

The previous works describes the investigation of various security issues that arise when "integrating wireless sensor networks into the IoT". It is difficult to find solutions that can achieve significant redcton in power consumption and still maintains system functionality and security [9, 10]. In our early studies, a heterogeneous offline and online encryption sstem was proposed for ensuring the security of communication data between internet host and sensor nodes. This paper demonstrates the scheme as indistinguishable from the "unselectable ciphertext attack in the bilinear Diffie-Hellman inversion problem and the q-strong Diffie-Hellman problem in the random oracle prediction model." The advantages of the proposed solution include achieving a good level of confidentiality, certification, non-repudiation, and integrity in a single and logical step. The system also allows message propagation from the sensor nodes in identity-based cryptography to the internet hosts through a public key system. Finally, te system considers two stages of encryption; these are offline and online ecryption phases. The offline phase permits offline heavy calculations without having to know the message, while the online phase permits only lightweight calculations when the message is accessible [11-14].

In WSN, size of transmitted data is directly related to energy consumption. Therefore, paper proposed an efficient hybrid model for ensuring the security of transmited data from the sensor nodes to the receivers via WSN. This study was conceived in a bid to discourage the use of data security algorithms for sensor data in situations whre the current sensor reading is equivalent to the transmitted value to the base station [15-17].

The contributions of this paper are as follows:

a) Development of a system that achieved integrity, confidentiality, certification, and non-repudiation in both single and logical steps.
b) Development of a syste that allows propagation o messages by sensor nodes in identity-based cryptography to the internet hosts in a public key infrastructure.
c) It avoids applying data security algorithms for sensor data when the current sensor reading is equal to the value sent to the base station.

This paper is organized into sections, Section 1 is a preface where the problem and the most important goals have been defined. Second section went through the studies related to the problem and discussed strengths and weaknesses of it. Third section spoke about the proposed system and included code, a diagram and mathematical equation, and fourth section discusses results and comparing them to algorithms exist and the last part is significance of statement and conclusion.

2. EFFICIENT DATA COLLECTION AND DISSEMINATION (EDCD)

A study by Li, F., & Xiong developed a method called EDCD1 for reducing the number of data propagation and amount of data to ensure extension of the service life of the network [18-20]. The proposed EDCD1 was based on the relative difference between the measured transmited values of the current sensor and the last sensor as defined in as shown in (1), where β is the maximum allowed differential value.

$$F_S = \begin{cases} If\ R_f = \frac{|V(t)-V(t-1)|}{V(t-1)} > \beta\ , 1 \\ Otherwise\ , 0 \end{cases} \quad (1)$$

```
Pseudo code for the EDCD1 algorithm as presented in [8]
EDCD1 Algorithm
Inputs
V(t),, V(t − 1), and β
Output
F_S: the binary parameter to send data / not send data
Begin
Set V(t − 1),← last measuring value transmitted by the sensor
Read: the sensor value (V) at t time
Set V(t),← V
//Calculate the relative change (R_f)
R_f=Abs (V(t) − V(t − 1),) / (V(t − 1))
If  R_f > β Then
Set F_S ← 1
Else: Set F_S ← 0
End if
// The decision to send data
If F_S = 1 Then
RFtransmit (ON) // Send the new data
Else: RFtransmit (Off) // No
End If
End Algorithm
```

The decision-making process in the EDCD1 relies on the relative difference value as shown in (1) based on a given threshold value of β for the update.

3. RSA ALGORITHM

The world today places much emphasis on data security owing to the advancement of the internet and the emergence of e-commerce, e-mail, online banking, and other services that have become a part of our daily lives. Despite the pleasure we derive from these services, they are also prone to privacy and security risks [21, 22]. As such, cryptography has been suggested as te ideal solution to these problems and many more [21, 23, 24]. Cryptography coms in differen formsbased on the number of keys employed; the tre major categories of cryptography are:

a) Secret key cryptography: Both encryption and decryption proceses are implemented using a single key.
b) Public key cryptography: A public key which is available to everyone is usd for the encryption process while the decryption processreqires a private/secret key which is available to only theintended recipient.
c) Hash functions: Here, an irreversible function is used to make information in the transmitted message un-retrievale from the original data; such systemsare used in mainly for securing data integrity [6, 25-28].

Pseudo code for RSA algorithm as described in [29]

RSA - Key generation
Select two distinct prime numbers p and q so that the product $n = pq$ has the required length.
Calculate $\varphi(n) = (p-1)(q-1)$.
Select a common exponent $e, 1 < e < \varphi(n)$, which is relatively prime to $\varphi(n), ie\ gcd(e, \varphi(n)) = 1$.
Calculate a private index d that satisfies $consensus \equiv 1\ (mod\ \varphi(n))$.
Make the public $key\ (n, e)$ available to others. Privacy privacy values $d, p, q, and\ \varphi(n)$.

RSA - Key generation
Rule- Encryption: ciphertext, $c = \boldsymbol{RsaPublic}(m) = m^e mod\ n, 1 < m < n-1$
Rule- Decryption: plaintext, $m = \boldsymbol{RsaPrivate}(c) = c^d\ mod\ n$
Inverse transformation: $m = \boldsymbol{RsaPrivate}(\boldsymbol{RsaPublic}(m))$

4. THE PROPOSED MODEL

This section described the proposed model. Figure 1 describes the general structure of the proposed model. The proposed model has two main stages: (i) EDCD1 and (ii) RSA. The septs of implementing the proposed model described in detail in the following Pseudocode.

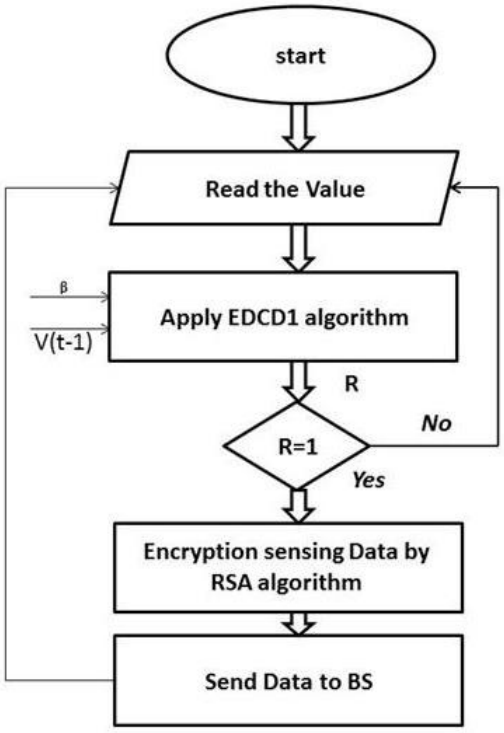

Figure 1. Flowchart proposed algorithm

PROPOSED MODEL
START:
INPUT: Real-time sensor value $V(t)$,
SET:
$\beta \leftarrow 0.01$, $P \leftarrow 33$ *and* $Q \leftarrow 54$,
APPLY EDCD1

$$F \leftarrow \boldsymbol{EDCD1}(V(t), V(t-1))$$

IF (F *NOT Equal Zero*) THEN
Encrypt the measured value by Apply RSA // Encryption measured data//
$C_{1\times n} \leftarrow \mathbf{RSA}\ (V(t), P, Q)$, $C \in R^{1\times n}$
SEND Data Encrypted $\boldsymbol{C_{1\times n}}$ TO the BS
Calculate the Energy consumption
SET $V(t) \leftarrow V(t-1)$
GO TO START
ELSE
No need to Encrypt the measured value
GO TO START
END IF
END ALGORITHM

5. RESUTS AND DISCUSSIONS

This section introduces the simulation and analysis study that used to test performance the proposed model. The assessment is based on numerous scenarios. The real-time data set used in this paper was extracted from the WSN deployment at Intel Berkeley Research Labs. Select a subset of this data set to evaluate the proposed model and MATLAB software was used for analysis. In this article, we assume that the cost of sending one byte is 59.2 uJ, as calculated for MICA2Dot mote.

The proposed model was evaluated in various scenarios as the follows, Figure 1 shown the Temperature sensor values in various forms floating point and integer, Figure 2 shown the Humidity sensor values in various forms floating point and integer and Figure 3 shown the Light sensor values in various forms floating point and integer. The parameters values set as shown in Table 1.

Figures 4, 5, 6 and 7 show the results of applying the provided model and RSA to real-time data sets with different types of sensors. It can be seen from the results that the proposed model shows better performance in terms of energy consumption. The total energy computations by applied RSA algorithm was higher than total energy computations by applied the proposed model in this article for all sensors temperatures, humidity, and light. The reason for that has RSA transmitted the chirper data for all samples which that increase the energy consumptions because the size of the cipher is such much large camper to the original data, especially for the sensors in floating point format as that clear from the results. For example, Figure 4 showed the cipher data for 3 samples for each value need 7 values after applied RSA to secure the transmitted data. Form the figure it observed that the cipher data2 and data3 are totally same, which that's mean the sensor node will waste the energy to transmit same chipper data for two consecutive samples. Conversely, the proposed model able to prevent secure sensed data if no significant change between the current data and the last transmitted data by the apply EDCD1 algorithm.

Table 1. Papramters values

Paramter	Value
Cost of sending one byte	59.2uJ
β	0.01
N the number of samples	500
q, p	37,51

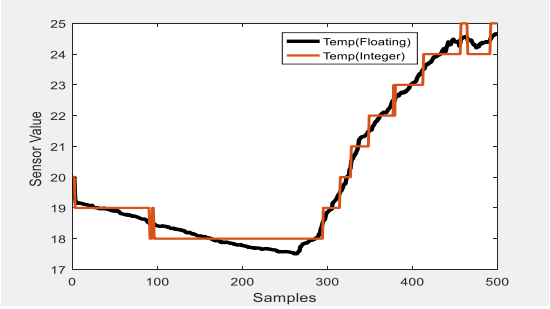

Figure 2. Temperature sensor values in various forms floating point and integer

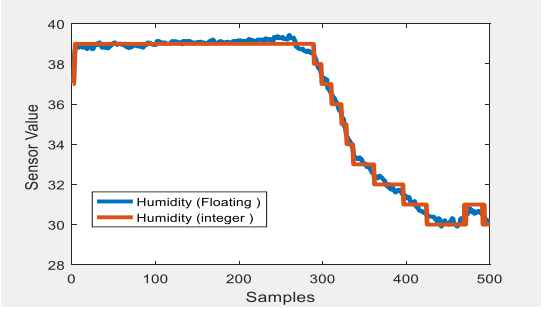

Figure 3. Humidity sensor values in various forms floating point and integer

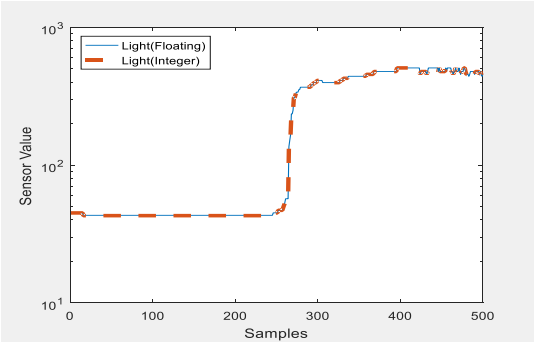

Figure 4. Light sensor values in various forms floating point and integer

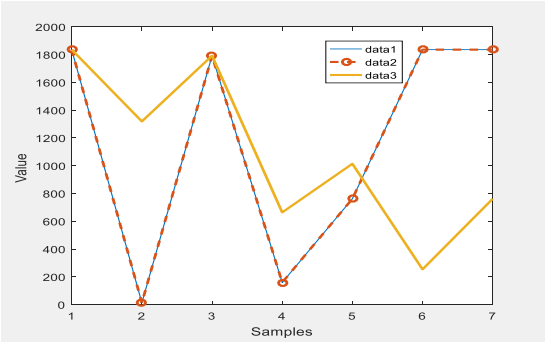

Figure 5. A Humidity sensor (cipher) transmitted

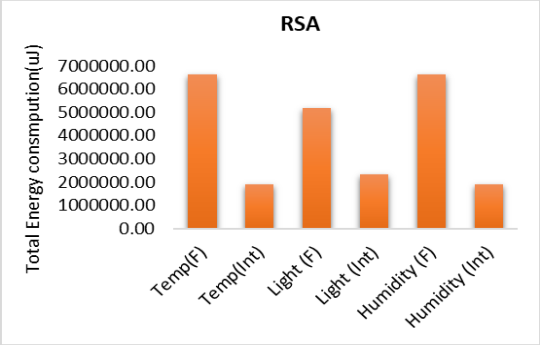

Figure 6. Total energy consumption by encryption sensing data (RSA)

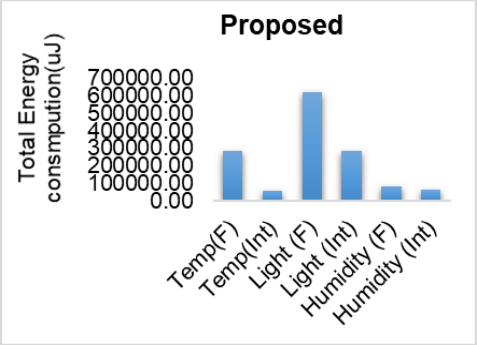

Figure 7. Total energy consumption by encryption sensing data (proposed)

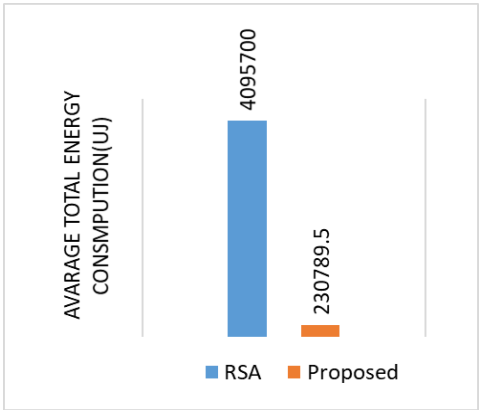

Figure 8. Average total energy consumption by encryption sensing data with RSA directly vs. proposed model

6. SIGNIFICANCE OF STATEMENT

This paper demonstrates the scheme as indistinguishable from the "unselectable ciphertext attack in the bilinear Diffie-Hellman inversion problem and the q-strong Diffie-Hellman problem in the random oracle prediction model." The advantages of the proposed solution include achieving a good level of confidentiality, certification, non-repudiation, and integrity in a single and logical step. The system also allows message propagation from the sensor nodes in identity-based cryptography to the internet hosts through a public key system. Finally, the system considers two stages of encryption; these are offline and online ecryption phases. The offline phase permits offline heavy calculations without having to know the message, while the online phase permits only lightweight calculations when the message is accesible.

7. CONCLUSION

In this paper, we proposed an efficient hybrid model for secure data propagation from the sensor nodes to the receivers via IoT-WSN platforms. The proposed model includes two algorithms RSA and EDCD1. The key idea behind the proposed model is to prevent secure sensed data if no significant change between the current data and the last transmitted data by apply EDCD algorithm, which that will help in saving the sensor node energy. The reason for that the size of cipher data is so large compared to the sensed data, which that will increase the energy consumption. The outcome results shown that the proposed model has a high performance compared to RSA in term of energy consumption.

REFERENCES

[1] R. A. Hasan and M. N. Mohammed, "A krill herd behaviour inspired load balancing of tasks in cloud computing," *Studies in Informatics and Control*, vol. 26, pp. 413-424, 2017.

[2] M. A. Mohammed, Z. H. Salih, N. Ţăpuş, and R. A. K. Hasan, "Security and accountability for sharing the data stored in the cloud," in *2016 15th RoEduNet Conference: Networking in Education and Research*, pp. 1-5, 2016.

[3] M. A. Mohammed and R. A. Hasan, "Particle swarm optimization for facility layout problems FLP—A comprehensive study," in *2017 13th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP)*, pp. 93-99, 2017.

[4] R. A. Hasan, M. A. Mohammed, N. Ţăpuş, and O. A. Hammood, "A comprehensive study: Ant Colony Optimization (ACO) for facility layout problem," in *2017 16th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1-8, 2017.

[5] R. A. Hasan, M. A. Mohammed, Z. H. Salih, M. A. B. Ameedeen, N. Ţăpuş, and M. N. Mohammed, "HSO: A Hybrid Swarm Optimization Algorithm for Reducing Energy Consumption in the Cloudlets," *Telkomnika*, vol. 16, pp. 2144-2154, 2018.

[6] N. Q. Mohammed, M. S. Ahmed, M. A. Mohammed, O. A. Hammood, H. A. N. Alshara, and A. A. Kamil, "Comparative Analysis between Solar and Wind Turbine Energy Sources in IoT Based on Economical and Efficiency Considerations," in *2019 22nd International Conference on Control Systems and Computer Science (CSCS)*, pp. 448-452, 2019.

[7] M. A. Mohammed, R. A. Hasan, M. A. Ahmed, N. Tapus, M. A. Shanan, M. K. Khaleel, *et al.*, "A Focal load balancer based algorithm for task assignment in cloud environment," in *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pp. 1-4, 2018.

[8] O. A. Hammood, M. N. M. Kahar, and M. N. Mohammed, "Enhancement the video quality forwarding Using Receiver-Based Approach (URBA) in Vehicular Ad-Hoc Network," in *2017 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET)*, pp. 64-67, 2017.

[9] M. A. Ahmed, R. A. Hasan, A. H. Ali, and M. A. Mohammed, "The classification of the modern arabic poetry using machine learning," *Telkomnika*, vol. 17, pp. 2667-2674, 2019.

[10] R. A. Hasan, I. Alhayali, A. Royida, N. D. Zaki, and A. H. Ali, "An adaptive clustering and classification algorithm for Twitter data streaming in Apache Spark," *Telkomnika*, vol. 17, 2019.

[11] R. A. Hasan, M. N. Mohammed, M. A. B. Ameedeen, and E. T. Khalaf, "Dynamic Load Balancing Model Based on Server Status (DLBS) for Green Computing," *Advanced Science Letters*, vol. 24, pp. 7777-7782, 2018.

[12] E. T. Khalaf, M. N. Mohammad, K. Moorthy, and R. A. Hasan, "Biometric Template Protection based on Hill Cipher Algorithm with Two Invertible keys," *Advanced Science Letters*, vol. 24, pp. 7643-7649, 2018.

[13] O. A. Hammood, M. N. M. Kahar, M. N. Mohammed, W. A. Hammood, and J. Sulaiman, "The VANET-Solution Approach for Data Packet Forwarding Improvement," *Advanced Science Letters*, vol. 24, pp. 7423-7427, 2018.

[14] O. A. Hammood, N. Nizam, M. Nafaa, and W. A. Hammood, "RESP: Relay Suitability-based Routing Protocol for Video Streaming in Vehicular Ad Hoc Networks," *International Journal of Computers, Communications & Control*, vol. 14, 2019.

[15] M. A. Mohammed, A. A. Kamil, R. A. Hasan, and N. Tapus, "An Effective Context Sensitive Offloading System for Mobile Cloud Environments using Support Value-based Classification," *Scalable Computing: Practice and Experience*, vol. 20, pp. 687-698, 2019.

[16] M. A. Mohammed, I. A. Mohammed, R. A. Hasan, N. Ţăpuş, A. H. Ali, and O. A. Hammood, "Green Energy Sources: Issues and Challenges," in *2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1-8, 2019.

[17] Z. F. Hussain, H. R. Ibraheem, M. Alsajri, A. Hussein Ali, M. A. Ismail, S. Kasim, *et al.*, "A new model for iris data set classification based on linear support vector machine parameter's optimization," *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 10, 2020.

[18] F. Li and P. Xiong, "Practical secure communication for integrating wireless sensor networks into the internet of things," *IEEE Sensors Journal*, vol. 13, pp. 3677-3684, 2013.

[19] N. D. Zaki, N. Y. Hashim, Y. M. Mohialden, M. A. Mohammed, T. Sutikno, and A. H. Ali, "A real-time big data sentiment analysis for iraqi tweets using spark streaming," *Bulletin of Electrical Engineering and Informatics*, vol. 9, pp. 1411-1419, 2020.

[20] H. R. Ibraheem, Z. F. Hussain, S. M. Ali, M. Aljanabi, M. A. Mohammed, and T. Sutikno, "A new model for large dataset dimensionality reduction based on teaching learning-based optimization and logistic regression," *Telkomnika*, vol. 18, 2020.

[21] O. A. Hammood, M. N. M. Kahar, W. A. Hammood, R. A. Hasan, M. A. Mohammed, A. A. Yoob, *et al.*, "An effective transmit packet coding with trust-based relay nodes in VANETs," *Bulletin of Electrical Engineering and Informatics*, vol. 9, pp. 685-697, 2020.
[22] H. D. K. Al-janabi, H. D. K. Al-janabi, and R. A. H. Al-Bukamrh, "Impact of Light Pulses Generator in Communication System Application by Utilizing Gaussian Optical Pulse," in *2019 22nd International Conference on Control Systems and Computer Science (CSCS)*, pp. 459-464, 2019.
[23] A. H. Ali and M. Z. Abdullah, "Recent trends in distributed online stream processing platform for big data: Survey," in *2018 1st Annual International Conference on Information and Sciences (AiCIS)*, pp. 140-145, 2018.
[24] M. A. Ahmed and S. Trausan-Matu, "Using natural language processing for analyzing Arabic poetry rhythm," in *2017 16th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1-5, 2017.
[25] S. I. Jasim, M. M. Akawee, and R. A. Hasan, "Spectrum sensing approaches in cognitive radio network," *Periodicals of Engineering and Natural Sciences*, vol. 7, pp. 1555-1562, 2019.
[26] Z. H. Salih, G. T. Hasan, and M. A. Mohammed, "Investigate and analyze the levels of electromagnetic radiations emitted from underground power cables extended in modern cities," in *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pp. 1-4, 2017.
[27] Z. H. Salih, G. T. Hasan, M. A. Mohammed, M. A. S. Klib, A. H. Ali, and R. A. Ibrahim, "Study the Effect of Integrating the Solar Energy Source on Stability of Electrical Distribution System," in *2019 22nd International Conference on Control Systems and Computer Science (CSCS)*, pp. 443-447, 2019.
[28] S. A.-b. Salman, A.-H. A. Salih, A. H. Ali, M. K. Khaleel, and M. A. Mohammed, "A New Model for Iris Classification Based on Naïve Bayes Grid Parameters Optimization," *International Journal of Sciences: Basic and Applied Research (IJSBAR)*, vol. 40, pp. 150-155, 2018.
[29] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," ed: Elsevier, 2018.